인증 관리

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/active-iq-unified-manager-918/config/task_edit_authentication_servers.html on November 13, 2026. Always check docs.netapp.com for the latest.

목차

인증 관리 . . . 1
- Active IQ Unified Manager에서 인증 서버 편집 . . . 1
- Active IQ Unified Manager에서 인증 서버 삭제 . . . 1
- Active IQ Unified Manager에서 Active Directory 또는 OpenLDAP으로 인증 . . . 1
- 감사 로깅 . . . 2
  - Active IQ Unified Manager의 감사 로그에 대해 알아보기 . . . 2
  - Active IQ Unified Manager 감사 로그 구성 . . . 3
  - Active IQ Unified Manager에서 감사 로그의 원격 로깅 활성화 . . . 3
- Active IQ Unified Manager의 원격 인증 페이지 사용 . . . 4
  - 인증 서버 영역 . . . 6

인증 관리

Active IQ Unified Manager에서 인증 서버 편집

Unified Manager 서버가 인증 서버와 통신하는 데 사용하는 포트를 변경할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 중첩 그룹 조회 사용 안 함 확인란을 선택하세요.
3. 인증 서버 영역에서 편집할 인증 서버를 선택한 다음 *편집*을 클릭합니다.
4. 인증 서버 편집 대화 상자에서 포트 세부 정보를 편집합니다.
5. *저장*을 클릭합니다.

Active IQ Unified Manager에서 인증 서버 삭제

Unified Manager 서버가 인증 서버와 통신하지 못하도록 하려면 인증 서버를 삭제할 수 있습니다. 예를 들어 관리 서버가 통신하는 인증 서버를 변경하려면 해당 인증 서버를 삭제하고 새 인증 서버를 추가하면 됩니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

인증 서버를 삭제하면 해당 인증 서버의 원격 사용자 또는 그룹은 더 이상 Unified Manager에 액세스할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 삭제할 인증 서버를 하나 이상 선택한 다음 *삭제*를 클릭하십시오.
3. 삭제 요청을 확인하려면 *예*를 클릭하세요.

   보안 연결 사용 옵션을 활성화하면 인증 서버와 연결된 인증서가 인증 서버와 함께 삭제됩니다.

Active IQ Unified Manager에서 Active Directory 또는 OpenLDAP으로 인증

관리 서버에서 원격 인증을 활성화하고 관리 서버가 인증 서버와 통신하도록 구성하면 인증 서버 내의 사용자가 Unified Manager에 액세스할 수 있습니다.

다음과 같은 사전 정의된 인증 서비스 중 하나를 사용하거나 사용자 지정 인증 서비스를 지정할 수 있습니다:

- Microsoft Active Directory

Microsoft Lightweight Directory Services를 사용할 수 없습니다.

- OpenLDAP

필요한 인증 서비스를 선택하고 적절한 인증 서버를 추가하여 인증 서버의 원격 사용자가 Unified Manager에 액세스할 수 있도록 설정할 수 있습니다. 원격 사용자 또는 그룹의 자격 증명은 인증 서버에서 관리됩니다. 관리 서버는 구성된 인증 서버 내의 원격 사용자를 인증하기 위해 Lightweight Directory Access Protocol(LDAP)을 사용합니다.

Unified Manager에서 생성된 로컬 사용자의 경우 관리 서버는 사용자 이름과 암호에 대한 자체 데이터베이스를 유지 관리합니다. 관리 서버는 인증을 수행하며 Active Directory 또는 OpenLDAP를 인증에 사용하지 않습니다.

감사 로깅

Active IQ Unified Manager의 감사 로그에 대해 알아보기

감사 로그를 사용하여 감사 로그가 손상되었는지 여부를 확인할 수 있습니다. 사용자가 수행한 모든 활동은 모니터링되어 감사 로그에 기록됩니다. 감사는 Active IQ Unified Manager의 모든 사용자 인터페이스 및 공개적으로 노출된 API 기능에 대해 수행됩니다.

*감사 로그: 파일 보기*를 사용하여 Active IQ Unified Manager에서 사용 가능한 모든 감사 로그 파일을 보고 액세스할 수 있습니다. 감사 로그: 파일 보기의 파일은 생성 날짜를 기준으로 나열됩니다. 이 보기에는 시스템의 설치 또는 업그레이드 시점부터 현재까지 캡처된 모든 감사 로그의 정보가 표시됩니다. Unified Manager에서 작업을 수행할 때마다 정보가 업데이트되며 로그에서 확인할 수 있습니다. 각 로그 파일의 상태는 로그 파일의 변조 또는 삭제를 감지하기 위해 적극적으로 모니터링되는 “File Integrity Status” 속성을 사용하여 캡처됩니다. 감사 로그가 시스템에서 사용 가능한 경우 감사 로그는 다음 상태 중 하나를 가질 수 있습니다.

상태	설명
활성	현재 로그가 기록되고 있는 파일입니다.
정상	시스템에 압축되어 저장되어 있는 비활성 파일입니다.
변조됨	사용자가 파일을 수동으로 편집하여 손상된 파일.
MANUAL_DELETE	권한 있는 사용자가 삭제한 파일입니다.
ROLLOVER_DELETE	롤링 구성 정책에 따른 롤오프로 인해 삭제된 파일입니다.
UNEXPECTED_DELETE	알 수 없는 이유로 삭제된 파일입니다.

감사 로그 페이지에는 다음과 같은 명령 버튼이 포함되어 있습니다:

- 구성
- 삭제
- 다운로드

DELETE 버튼을 사용하면 감사 로그 보기에 나열된 감사 로그를 삭제할 수 있습니다. 감사 로그를 삭제할 수 있으며, 선택적으로 파일 삭제 사유를 제공할 수 있어 향후 유효한 삭제인지 판단하는 데 도움이 됩니다. REASON 열에는 삭제 작업을 수행한 사용자의 이름과 함께 사유가 표시됩니다.

로그 파일을 삭제하면 시스템에서 파일이 삭제되지만 DB 테이블의 항목은 삭제되지 않습니다.

Active IQ Unified Manager의 감사 로그 섹션에서 다운로드 버튼을 사용하여 감사 로그를 다운로드하고 감사 로그 파일을 내보낼 수 있습니다. “NORMAL” 또는 "`TAMPERED`"로 표시된 파일은 압축된 `.gzip` 형식으로 다운로드됩니다.

감사 로그 파일은 주기적으로 보관되어 참조를 위해 데이터베이스에 저장됩니다. 보관하기 전에 보안 및 무결성 유지를 위해 감사 로그에 디지털 서명이 적용됩니다.

전체 AutoSupport 번들이 생성될 경우, 지원 번들에는 보관된 감사 로그 파일과 활성 감사 로그 파일이 모두 포함됩니다. 하지만 간소화된 지원 번들이 생성될 경우에는 활성 감사 로그만 포함됩니다. 보관된 감사 로그는 포함되지 않습니다.

Active IQ Unified Manager 감사 로그 구성

감사 로그 섹션의 구성 버튼을 사용하여 감사 로그 파일에 대한 롤링 정책을 구성하고 감사 로그에 대한 원격 로깅을 활성화할 수 있습니다.

시스템에 저장할 데이터의 양과 빈도에 따라 최대 파일 크기 및 감사 로그 보존 기간(일)*의 값을 설정할 수 있습니다. *총 감사 로그 크기 필드의 값은 시스템에 있는 전체 감사 로그 데이터의 크기입니다. 롤오버 정책은 감사 로그 보존 기간(일), 최대 파일 크기 및 총 감사 로그 크기 필드의 값에 따라 결정됩니다. 감사 로그 백업 크기가 총 감사 로그 크기*에 구성된 값에 도달하면 가장 먼저 아카이브된 파일이 삭제됩니다. 즉, 가장 오래된 파일이 삭제됩니다. 하지만 파일 항목은 데이터베이스에서 계속 사용할 수 있으며 **"`Rollover Delete`"**로 표시됩니다. *감사 로그 보존 기간(일) 값은 감사 로그 파일이 보존되는 일수입니다. 이 필드에 설정된 값보다 오래된 파일은 롤오버됩니다.

단계

1. 감사 로그 > > *구성*을 클릭합니다.
2. 최대 파일 크기, 총 감사 로그 크기, *감사 로그 보존 기간(일)*에 값을 입력하십시오.

   원격 로깅을 활성화하려면 *원격 로깅 활성화*를 선택하십시오.

Active IQ Unified Manager에서 감사 로그의 원격 로깅 활성화

감사 로그 구성 대화 상자에서 원격 로깅 사용 확인란을 선택하여 원격 감사 로깅을 활성화할 수 있습니다. 이 기능을 사용하여 감사 로그를 원격 Syslog 서버로 전송할 수 있습니다. 이를 통해 공간 제약이 있는 경우 감사 로그를 관리할 수 있습니다.

감사 로그의 원격 로깅은 Active IQ Unified Manager 서버의 감사 로그 파일이 변조될 경우를 대비하여 변조 방지 백업을 제공합니다.

단계

1. 감사 로그 구성 대화 상자에서 원격 로깅 사용 확인란을 선택합니다.

   원격 로깅을 구성하기 위한 추가 필드가 표시됩니다.

2. 연결하려는 원격 서버의 **HOSTNAME** 및 **PORT** 를 입력합니다.
3. **SERVER CA CERTIFICATE** 필드에서 **BROWSE** 를 클릭하여 대상 서버의 공개 인증서를 선택합니다.

   인증서는 `.pem` 형식으로 업로드해야 합니다. 이 인증서는 대상 Syslog 서버에서 발급받아야 하며 만료되지 않은 것이어야 합니다. 인증서에는 선택한 "`hostname`"이 `SubjectAltName` (SAN) 속성의 일부로 포함되어 있어야 합니다.

4. 다음 필드의 값을 입력하십시오: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   이 필드들의 값은 밀리초 단위여야 합니다.

5. **FORMAT** 및 **PROTOCOL** 필드에서 필요한 Syslog 형식과 TLS 프로토콜 버전을 선택하십시오.
6. 대상 Syslog 서버에서 인증서 기반 인증이 필요한 경우 클라이언트 인증 사용 확인란을 선택하십시오.

   감사 로그 구성을 저장하기 전에 클라이언트 인증 인증서를 다운로드하여 Syslog 서버에 업로드해야 합니다. 그렇지 않으면 연결이 실패합니다. Syslog 서버의 유형에 따라 클라이언트 인증 인증서의 해시를 생성해야 할 수도 있습니다.

   예: syslog-ng는 명령 `openssl x509 -noout -hash -in cert.pem`을 사용하여 인증서의 <hash>을 생성해야 하며, 그런 다음 클라이언트 인증 인증서를 <hash> .0이라는 이름의 파일에 심볼릭 링크해야 합니다.

7. 서버와의 연결을 구성하고 원격 로깅을 활성화하려면 *저장*을 클릭하십시오.

   감사 로그 페이지로 리디렉션됩니다.

> ⓘ 연결 시간 초과 값은 구성에 영향을 미칠 수 있습니다. 구성이 응답하는 데 정의된 값보다 시간이 더 오래 걸리면 연결 오류로 인해 구성이 실패할 수 있습니다. 성공적인 연결을 설정하려면 연결 시간 초과 값을 늘리고 구성을 다시 시도하십시오.

Active IQ Unified Manager의 원격 인증 페이지 사용

원격 인증 페이지를 사용하여 Unified Manager가 인증 서버와 통신하도록 구성하고 Unified Manager 웹 UI에 로그인하려는 원격 사용자를 인증할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

'원격 인증 사용' 확인란을 선택한 후 인증 서버를 사용하여 원격 인증을 활성화할 수 있습니다.

- 인증 서비스

  Active Directory, OpenLDAP 등 디렉터리 서비스 공급자에서 사용자를 인증하도록 관리 서버를 구성하거나 자체 인증 메커니즘을 지정할 수 있습니다. 원격 인증을 활성화한 경우에만 인증 서비스를 지정할 수 있습니다.

  - **Active Directory**
    - 관리자 이름

      인증 서버의 관리자 이름을 지정합니다.

    - 비밀번호

      인증 서버에 접속하기 위한 비밀번호를 지정합니다.

    - 기본 고유 이름

      인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com+인 경우 기본 고유 이름은 *cn=ou,dc=domain,dc=com*입니다.

- 중첩 그룹 조회 비활성화

  중첩 그룹 조회 옵션을 활성화할지 비활성화할지 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩 그룹 지원을 비활성화하면 인증 속도를 높일 수 있습니다.

- 보안 연결 사용

  인증 서버와의 통신에 사용되는 인증 서비스를 지정합니다.

◦ **OpenLDAP**

- 바인드 고유 이름

  인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인드 고유 이름을 지정합니다.

- 바인드 비밀번호

  인증 서버에 접속하기 위한 비밀번호를 지정합니다.

- 기본 고유 이름

  인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com+인 경우 기본 고유 이름은 *cn=ou,dc=domain,dc=com*입니다.

- 보안 연결 사용

  LDAP 인증 서버와의 통신에 보안 LDAP를 사용한다고 명시합니다.

◦ 기타

- 바인드 고유 이름

  구성된 인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인드 고유 이름을 지정합니다.

- 바인드 비밀번호

  인증 서버에 접속하기 위한 비밀번호를 지정합니다.

- 기본 고유 이름

  인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com+인 경우 기본 고유 이름은 *cn=ou,dc=domain,dc=com*입니다.

- 프로토콜 버전

  인증 서버에서 지원하는 LDAP(Lightweight Directory Access Protocol) 버전을 지정합니다. 프로토콜 버전을 자동으로 감지할지 여부를 지정하거나 버전을 2 또는 3으로 설정할 수 있습니다.

- 사용자 이름 속성

  관리 서버에서 인증할 사용자 로그인 이름이 포함된 인증 서버의 속성 이름을 지정합니다.

- 그룹 멤버십 속성

  사용자 인증 서버에 지정된 속성 및 값을 기반으로 원격 사용자에게 관리 서버 그룹 멤버십을 할당하는 값을 지정합니다.

- UGID

  원격 사용자가 인증 서버의 GroupOfUniqueNames 오브젝트의 구성원으로 포함된 경우, 이 옵션을 사용하면 해당 GroupOfUniqueNames 오브젝트의 지정된 속성을 기반으로 원격 사용자에게 관리 서버 그룹 멤버십을 할당할 수 있습니다.

- 중첩 그룹 조회 비활성화

  중첩 그룹 조회 옵션을 활성화할지 비활성화할지 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩 그룹 지원을 비활성화하면 인증 속도를 높일 수 있습니다.

- 멤버

  인증 서버가 그룹의 개별 구성원에 대한 정보를 저장하는 데 사용하는 속성 이름을 지정합니다.

- 사용자 오브젝트 클래스

  원격 인증 서버에서 사용자의 오브젝트 클래스를 지정합니다.

- 그룹 오브젝트 클래스

  원격 인증 서버에 있는 모든 그룹의 오브젝트 클래스를 지정합니다.

  > *Member*, *User* 오브젝트 *Class*, *Group* 오브젝트 *Class* 속성에 입력하는 값은 Active Directory, OpenLDAP 및 LDAP 구성에 추가된 값과 동일해야 합니다. 그렇지 않으면 인증에 실패할 수 있습니다.

- 보안 연결 사용

  인증 서버와의 통신에 사용되는 인증 서비스를 지정합니다.

> 인증 서비스를 수정하려면 기존 인증 서버를 모두 삭제하고 새 인증 서버를 추가해야 합니다.

인증 서버 영역

인증 서버 영역에는 관리 서버가 원격 사용자를 찾고 인증하기 위해 통신하는 인증 서버가 표시됩니다. 원격 사용자 또는 그룹의 자격 증명은 인증 서버에서 관리합니다.

- 명령 버튼

  인증 서버를 추가, 편집 또는 삭제할 수 있습니다.

  - 추가

    인증 서버를 추가할 수 있습니다.

  추가하려는 인증 서버가 고가용성 쌍(동일한 데이터베이스 사용)의 일부인 경우 파트너 인증 서버도 추가할 수

있습니다. 이렇게 하면 인증 서버 중 하나에 연결할 수 없는 경우에도 관리 서버가 파트너와 통신할 수 있습니다.

  - 편집

    선택한 인증 서버의 설정을 편집할 수 있습니다.

  - 삭제

    선택한 인증 서버를 삭제합니다.

- 이름 또는 **IP** 주소

  관리 서버에서 사용자를 인증하는 데 사용되는 인증 서버의 호스트 이름 또는 IP 주소를 표시합니다.

- 포트

  인증 서버의 포트 번호를 표시합니다.

- 인증 테스트

  이 버튼은 원격 사용자 또는 그룹을 인증하여 인증 서버의 구성을 확인합니다.

  테스트 중에 사용자 이름만 지정하면 관리 서버는 인증 서버에서 원격 사용자를 검색하지만 인증은 수행하지 않습니다. 사용자 이름과 암호를 모두 지정하면 관리 서버는 원격 사용자를 검색하고 인증합니다.

  원격 인증이 비활성화된 경우 인증 테스트를 수행할 수 없습니다.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.